

HP ProLiant Essentials Vulnerability and Patch Management Pack Server Security Recommendations

Security Considerations for VPM and HP SIM Servers



Introduction	3
External patch acquisition	4
Comparing logical and physical configurations	4
Single-node configuration	6
Distributed configuration	6
HP SIM credentials	7
VPM server credentials	8
SSL certificates	9
Removing the SSL certificate	10
Security recommendations for both configurations	13
Removal of the OpenSSH dependency	13
Setting Windows file protections	14
Limiting remote file shares	15
Firewalls and DMZs	16
Configuration A	16
Configuration B	18
Configuration C	19
Vulnerability and Patch Management Pack firewall ports	20
HP SIM server	20
VPM server	20
MSDE	20
Harris STATScanner Engine	20
Radia Patch Manager	20
Target nodes	21
Scanner access (target nodes)	21
HP SIM	21
Radia Patch Manager	21

Security relationship between Vulnerability and Patch Management Pack and target systems	21
Vulnerability scan security	22
Patch security	22
Configuration fix security	22
Vulnerability and Patch Management Pack patching and the Windows XP SP2 firewall	22
For more information	23

Introduction

The HP ProLiant Essentials Vulnerability and Patch Management (VPM) server is the logical server that houses both the HP Systems Insight Manager (HP SIM) and Vulnerability and Patch Management Pack software. Although HP SIM and Vulnerability and Patch Management Pack can be located on separate physical servers to provide improved scaling and performance, for security purposes carefully treat both programs as a whole, rather than treating the individual applications as separate entities.

With the release of version 1.10, you can also distribute the patch acquisition task to yet another Microsoft Windows machine, which has access to vendors patch feeds. Consider the entire HP SIM/VPM entity, consisting of the full combination of management and security information, vulnerabilities, and credentials, when establishing security from external interference.

The combined HP SIM/VPM environment houses many key security tokens or credentials, allowing Vulnerability and Patch Management Pack to effectively scan and patch security vulnerabilities. For this reason, HP recommends certain precautionary configuration steps to ensure that the sensitive information remains uncompromised.

The following is an overview of the recommended precautionary configuration:

- Treat the security environment of the HP SIM/VPM entity as one, instead of three separate systems. Distributing the applications among three systems can reduce the amount of traffic that must pass through firewalls and the possibility of false alarms in network management applications. However, the distributed configuration over an open network can create opportunities for security breaches or application failures caused by password expiration and coordination, network spoofing, or man-in-the-middle attacks. This configuration also requires more maintenance when passwords change, certificates expire, or administrative rights are updated. Use of the VPM Acquisition Utility is optional and can be used with both the distributed and single-node configurations. For simplicity, HP recommends installing all components of the HP SIM/VPM environment on a single physical server. This configuration reduces the amount of network traffic and administrative coordination between the application components, thereby reducing potential attacks.
- Reduce the number of local and remote user accounts in the HP SIM/VPM environment to a minimum, limiting the exposure of sensitive management data (primarily, the credentials used for security scanning and patching).
- Enable Secure Sockets Layer (SSL) Certificate Services in Microsoft Internet Information Services (IIS) for the VPM server, creating an HTTPS communication channel between Vulnerability and Patch Management Pack and HP SIM.
- Enable firewalls and demilitarized zones (DMZs) for Vulnerability and Patch Management Pack usage when exposing a private network to public Internet access points. Limit exposure to sensitive systems appropriately with a variety of levels of security access. A layered approach is often preferred.
- Secure the security relationship between Vulnerability and Patch Management Pack and its targets.

=====

External patch acquisition

With the advent of Vulnerability and Patch Management Pack 1.10, you can now break out patch acquisition to another Windows system. The main purposes of this functionality is to allow the download of patches to occur in an environment that is exposed to the Internet and allow the resulting patch repository to be imported into the VPM server through a VPM patch import mechanism. You should allow the acquisition to occur in a controlled, external environment with access to software vendors' patch feed (for example, Red Hat and Microsoft). When the acquisition is complete, patches should be scanned with the usual file virus scanners, transferred into your VPM server repository environment, and then imported into VPM for patch evaluation and testing. After testing, the patches should then be applied to target systems that have these vulnerabilities.

Comparing logical and physical configurations

The Vulnerability and Patch Management Pack plug-in for HP SIM can be configured on:

- A single x86 Microsoft Windows server
- Two separate x86 Windows servers connected using a TCP/IP LAN

Figure 1. A single-node configuration

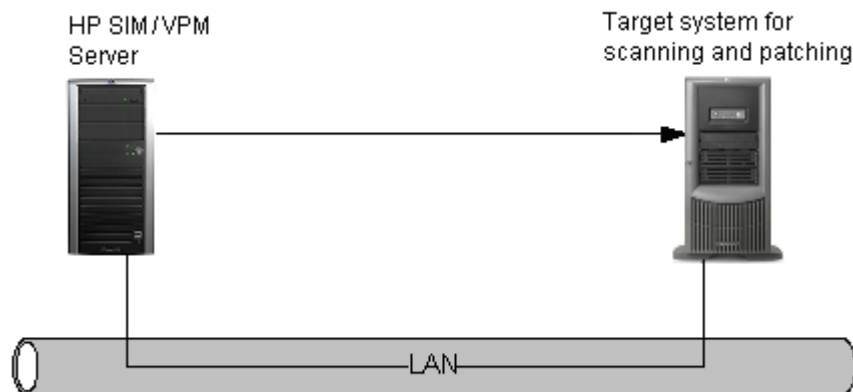


Figure 2. A single-node configuration with the VPM Acquisition Utility

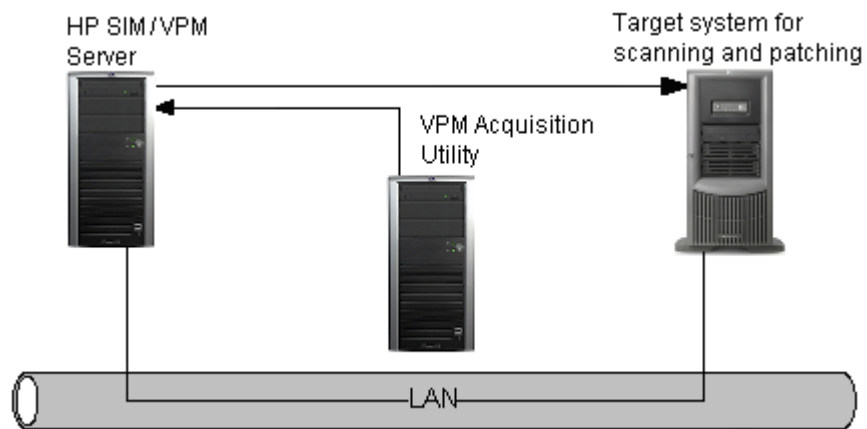


Figure 3. A distributed configuration across two systems

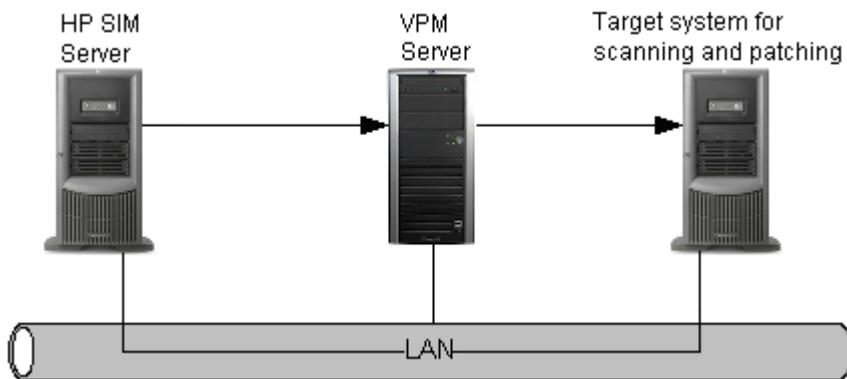
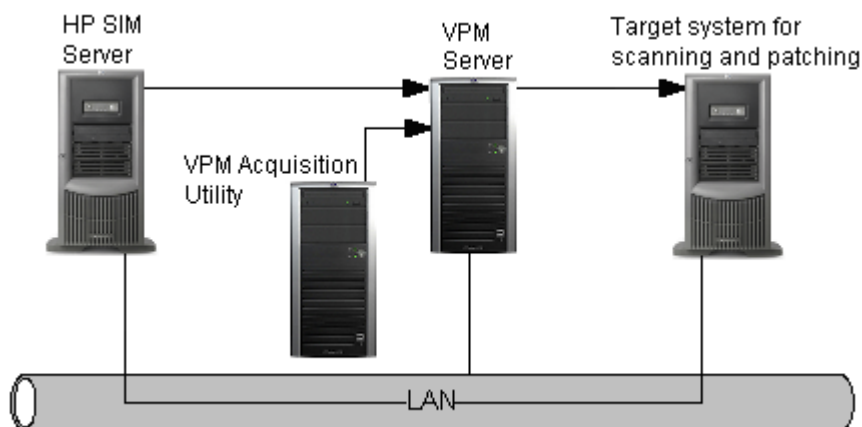


Figure 4. A distributed configuration across three systems with the VPM Acquisition Utility



Single-node configuration

Installing HP SIM and Vulnerability and Patch Management Pack on a single server greatly simplifies the security configuration by keeping all components on a single host, eliminating any system requests and responses over the open network. Credential coordination, although necessary between applications, does not have to extend beyond the boundaries of the single hosting system.

If you do not have the server capacity to operate and maintain both the HP SIM and Vulnerability and Patch Management Pack applications on a single server or if it is necessary for the VPM server to be located in the DMZ so it has Internet accessibility, you can split these applications by migrating to a distributed server configuration.

The VPM Acquisition Utility is optional and can be used with both the distributed and single-node configurations.

Distributed configuration

When HP SIM and the Vulnerability and Patch Management Pack create too great of a load for a single system or when it is necessary for the VPM server to be in the DMZ to access patches and updates from the Internet, each component can be installed on separate systems, with the vulnerability scanning and patching functions relegated to a second host system. In this distributed configuration, additional security settings should be established and synchronized across applications before their installation. These security settings consist of:

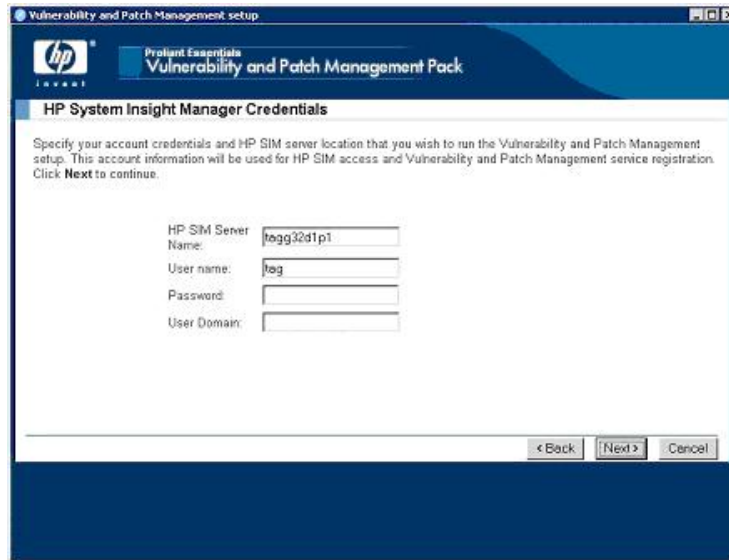
- HP SIM server credentials used by Vulnerability and Patch Management Pack
- VPM server credentials used by HP SIM for Vulnerability and Patch Management Pack operations
- The VPM server SSL certificate

The current Vulnerability and Patch Management Pack installation automatically establishes the HP SIM and VPM server credentials, but enabling the SSL certificate should be performed manually before installing the Vulnerability and Patch Management Pack. After the SSL certificate is correctly installed, the Vulnerability and Patch Management Pack installation recognizes this and can enable usage without further configuration.

HP SIM credentials

During the Vulnerability and Patch Management Pack installation, HP SIM credentials must be entered at the following screen. Entering your HP SIM credentials allows Vulnerability and Patch Management Pack to obtain essential account information necessary to gain access to and respond to requests from HP SIM.

Figure 5. HP SIM credentials

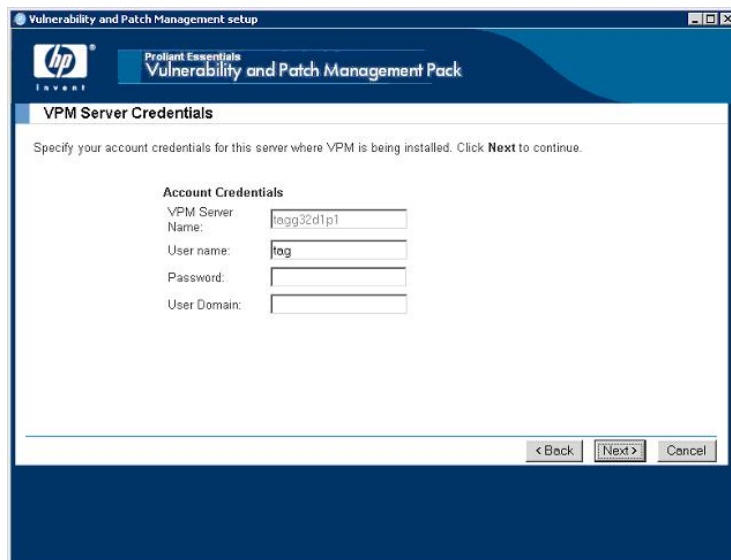


The screenshot shows a Windows-style window titled "Vulnerability and Patch Management setup". The window has a blue header bar with the HP logo and the text "Proant Essentials Vulnerability and Patch Management Pack". Below the header, the title bar reads "HP System Insight Manager Credentials". The main content area contains the following text: "Specify your account credentials and HP SIM server location that you wish to run the Vulnerability and Patch Management setup. This account information will be used for HP SIM access and Vulnerability and Patch Management service registration. Click **Next** to continue." Below this text are four input fields: "HP SIM Server Name:" with the value "l0gg32d1p1", "User name:" with the value "l0g", "Password:" (empty), and "User Domain:" (empty). At the bottom right of the window are three buttons: "< Back", "Next >", and "Cancel".

VPM server credentials

When the Vulnerability and Patch Management Pack installation prompts for the HP SIM server name, entering a remote HP SIM system indicates a distributed configuration. A distributed configuration requires that the VPM server credentials be entered at the following screen to allow HP SIM to communicate with the VPM server. Therefore, when a Vulnerability and Patch Management Patch scan or patch operation is requested, these credentials are used.

Figure 6. VPM server configurations



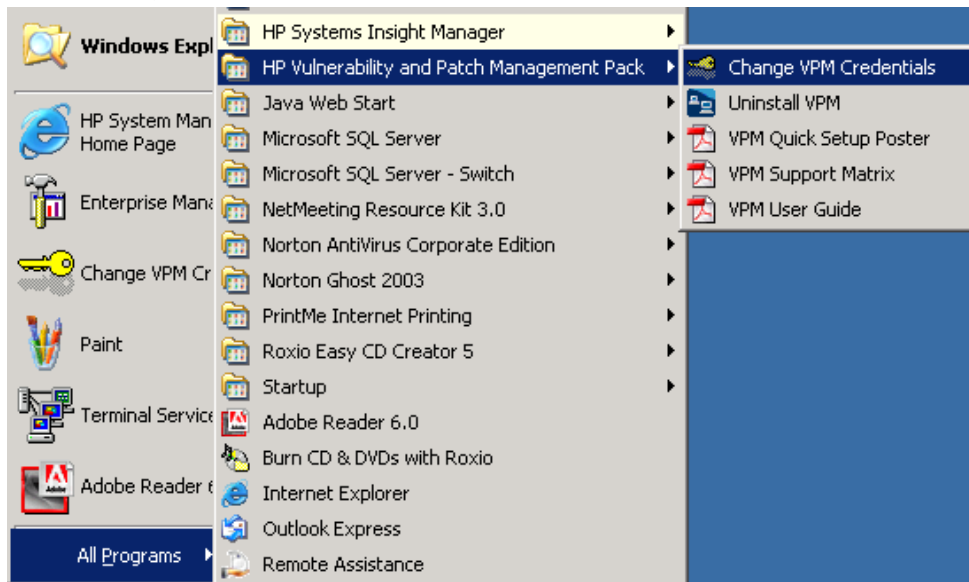
Note: Both sets of credentials are stored encrypted in various configuration files. The application directories for HP SIM and Vulnerability and Patch Management Pack must have administrative file protections. First, protect the directories and files from the local user community, allowing only the appropriate administrator access. Next, restrict remote shares and remote access to the appropriate administrative users (from a restricted list of systems). Finally, reduce the chances of vulnerability penetration by reducing the administrative or privileged groups to the smallest possible number of users. For instructions, refer to the “Security recommendations for both configurations” section.

SSL certificates

- Enabling the HP SIM Trust by SSL certificate option—in a distributed configuration, an extra level of access control can be enabled in HP SIM to allow connections only from certain systems, depending on the acquisition and deployment of SSL certificates. For more information, refer to *Understanding HP Systems Insight Manager Security* in the HP SIM Information Library at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html#whitepapers>
- Installing the VPM server SSL certificate—in the distributed environment, requests for Vulnerability and Patch Management Pack actions from HP SIM should be protected with an HTTPS link. Ensure that the HTTPS link is established by placing an SSL certificate in the IIS Web service certificate store. Apply the certificate to the STATScanner website **Properties**.

For more information, refer to either of the following sources:

- <http://msdn.microsoft.com/library/default.asp?url=/library/en-s/secmod/html/secmod30.asp>
 - <http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/maintain/featusability/c06iis.msp>
- Adding the SSL certificate after the initial installation—if Vulnerability and Patch Management Pack is initially installed without the SSL certificate, it can be added later. To communicate the configuration change to Vulnerability and Patch Management Pack:
 - a. Select **Start>All Programs>HP Vulnerability and Patch Management Pack>Change VPM Credentials**.



- b. Select the **Use secure connection when connecting to VPM server** checkbox to change the setting from insecure (HTTP) to secure (HTTPS) mode, utilizing the advantage of the SSL certificate.
- c. Click **Change**.

Change VPM Credentials Utility

SIM Server:
tagg32d1p1

User name:
Administrator

Domain:
TAGG32D1P1

Old Password:
[Empty]

New Password:
[Empty]

Confirm New Password:
[Empty]

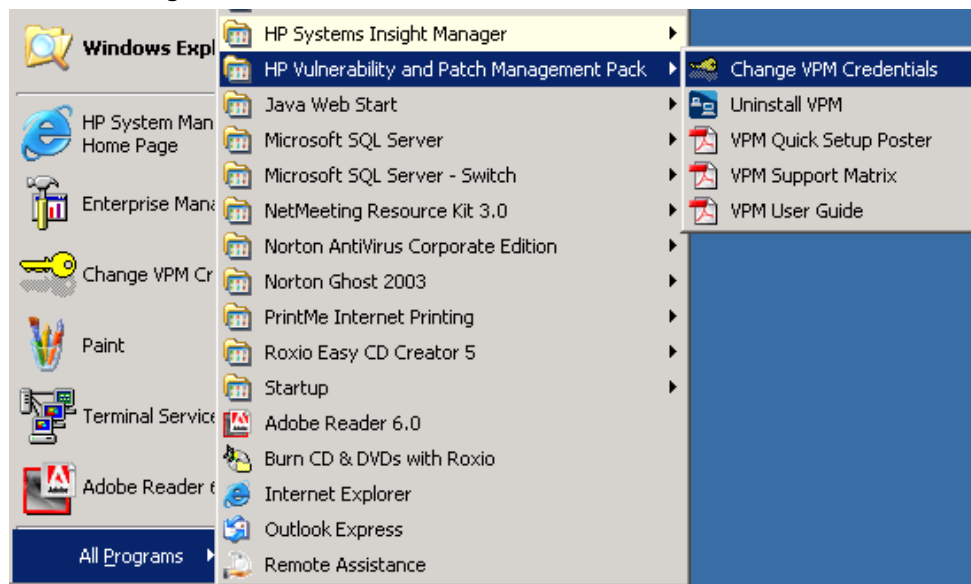
☒ Use secure connection when connecting to VPM server

Change Cancel

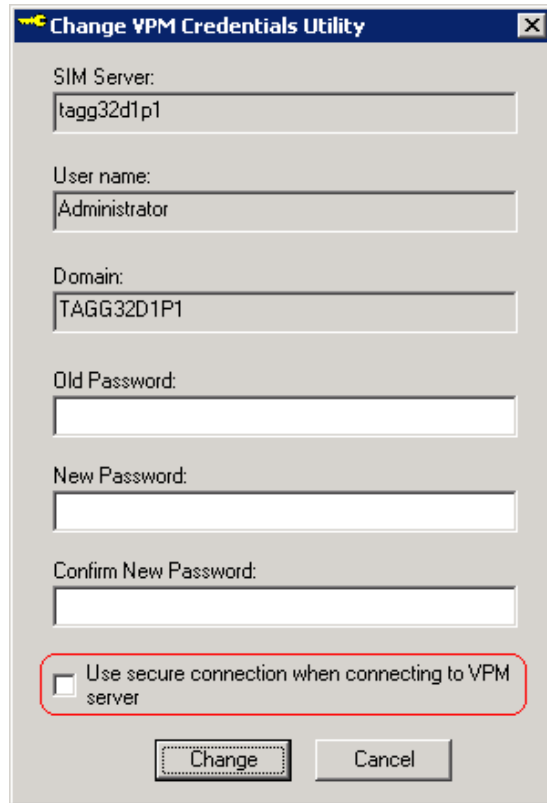
Removing the SSL certificate

HP does not recommend lowering the security level of the HP SIM/VPM configuration. However, the SSL certificate can be removed using the following steps:

1. Modify settings using the Change VPM Credentials Utility.
 - a. Select **Start>All Programs>HP Vulnerability and Patch Management Pack>Change VPM Credentials**.



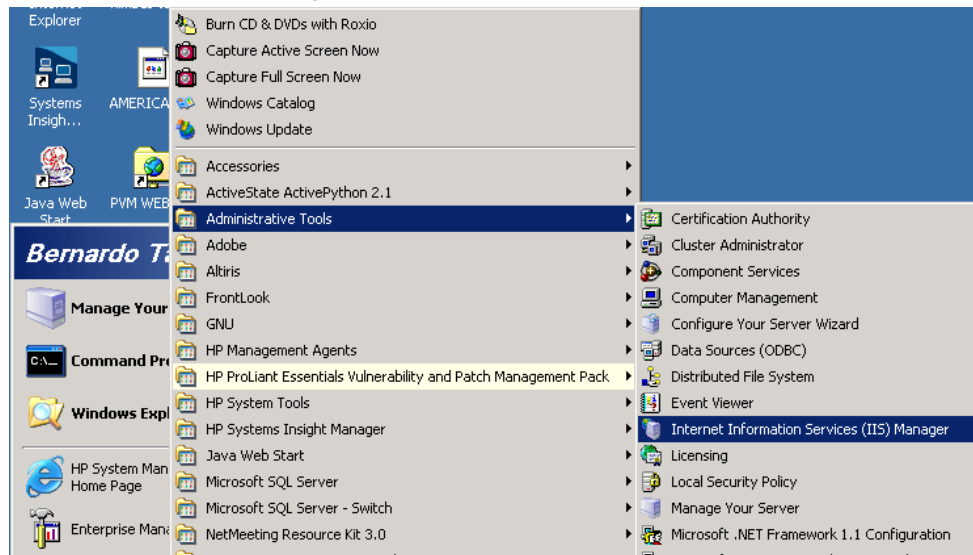
- b. Deselect the **Use secure connection when connecting to VPM server** checkbox.
- c. Click **Change**.



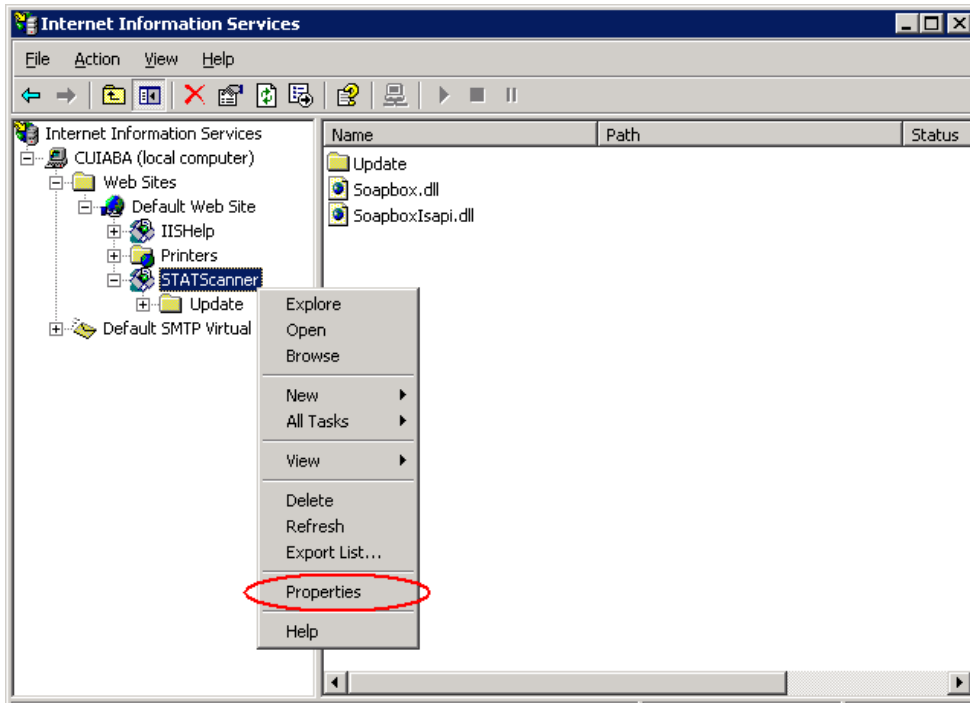
The image shows a Windows dialog box titled "Change VPM Credentials Utility". It contains several text input fields and a checkbox. The fields are labeled: "SIM Server:" with the value "tagg32d1p1", "User name:" with the value "Administrator", "Domain:" with the value "TAGG32D1P1", "Old Password:", "New Password:", and "Confirm New Password:". Below these fields is a checkbox labeled "Use secure connection when connecting to VPM server", which is currently unchecked and highlighted with a red rectangle. At the bottom of the dialog are two buttons: "Change" and "Cancel".

2. Enter the IIS administrator.

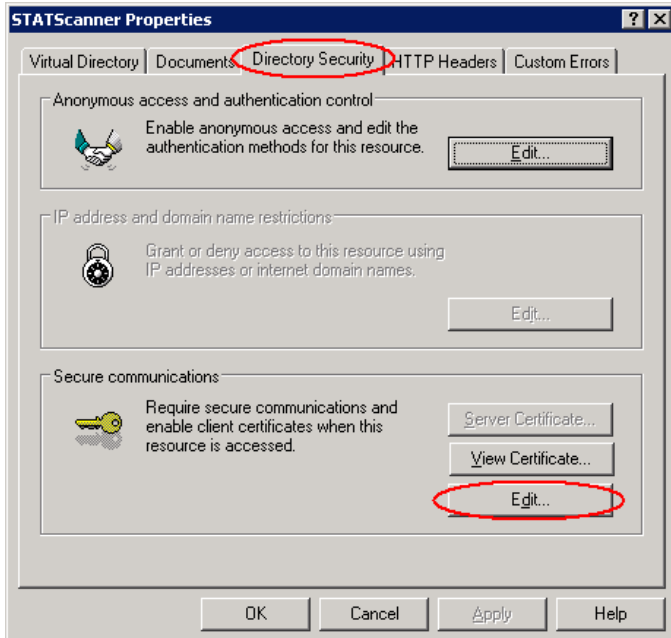
- a. Select **Start>All Programs>Administrative Tools>Internet Information Services (IIS) Manager**.



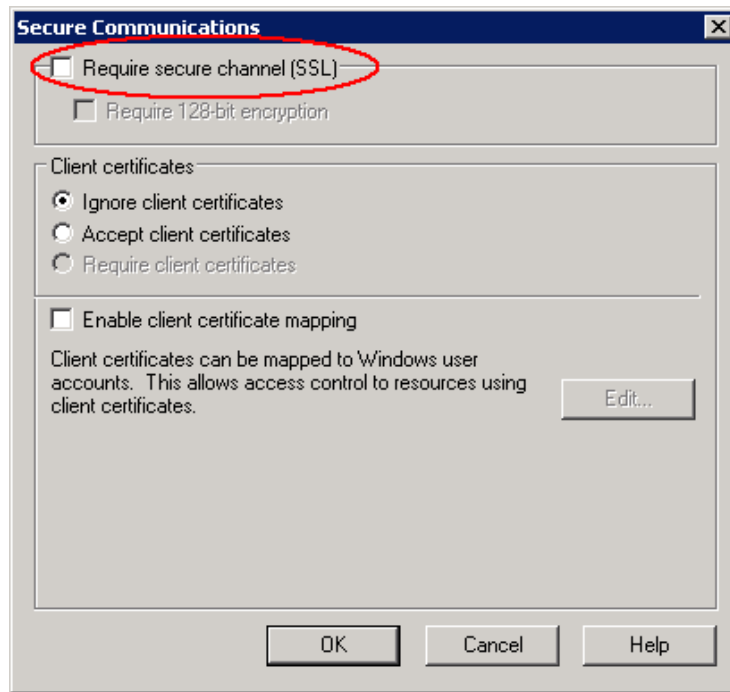
- b. Expand the local computer directory.
- c. Expand the **Web Sites** directory.
- d. Expand the **Default Web Site** directory.
- e. Right-click the **STATScanner** website and select **Properties**.



- f. Click the **Directory Security** tab, and click **Edit**.



- g. Deselect the **Require secure channel (SSL)** checkbox, and click **OK>Apply**.



Security recommendations for both configurations

The following sections detail some general security recommendations applicable to both the single-node and distributed configurations.

Removal of the OpenSSH dependency

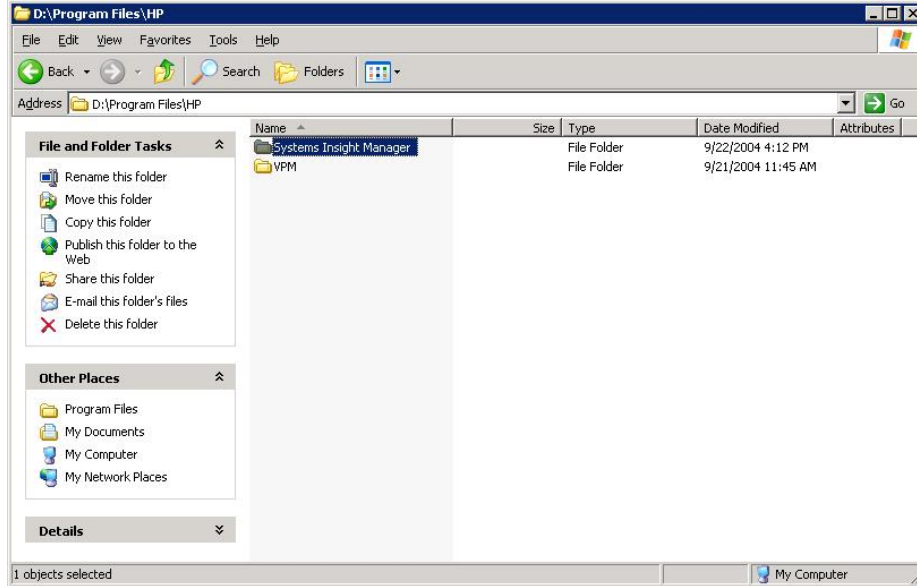
With HP SIM 4.2 SP2 and later, the OpenSSH configuration is no longer a requirement for Vulnerability and Patch Management Pack.

Setting Windows file protections

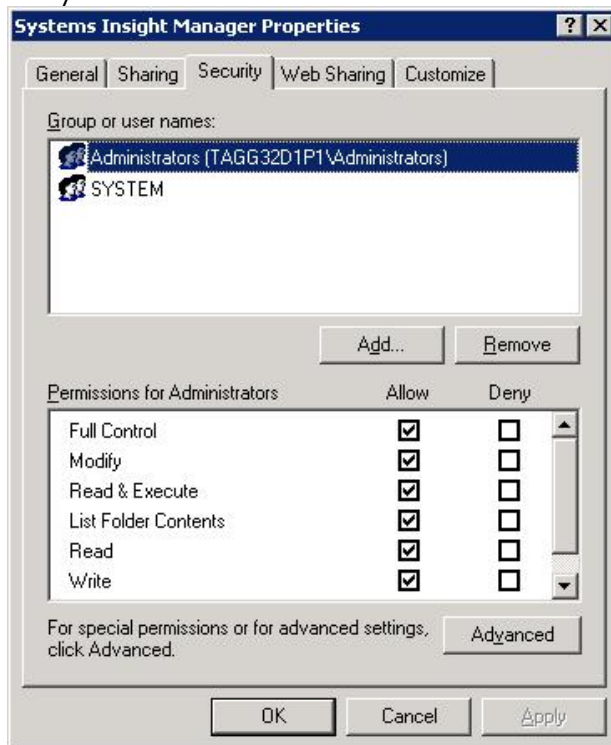
The HP SIM installation requires that the HP SIM files be retained in an NTFS partition. Vulnerability and Patch Management Pack must also be installed on an NTFS partition to ensure sufficient file system capabilities to secure sensitive directories. Normally, the HP SIM installation sets up the correct protections. However, in some environments, these file protections might require modification.

To set the correct file protection:

1. Access the C:\Program Files\HP directory.



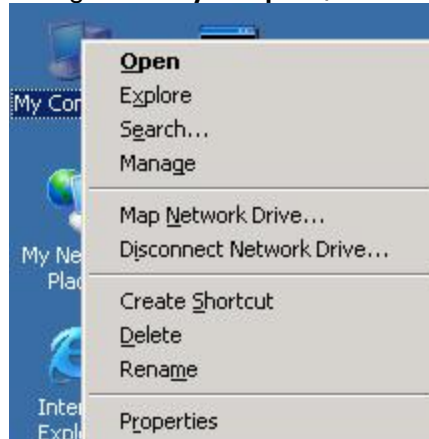
2. Set the file properties in both the VPM and Systems Insight Manager directories as restrictively as possible, while still enabling the applications to run. Properties can vary depending on the account used for the HP SIM installation, which is the account used to run the HP SIM service. As illustrated in the following figure, the system, TAGG32D1P1, can be accessed by only two accounts: members of the local system Administrators group (used during installation) and the System account.



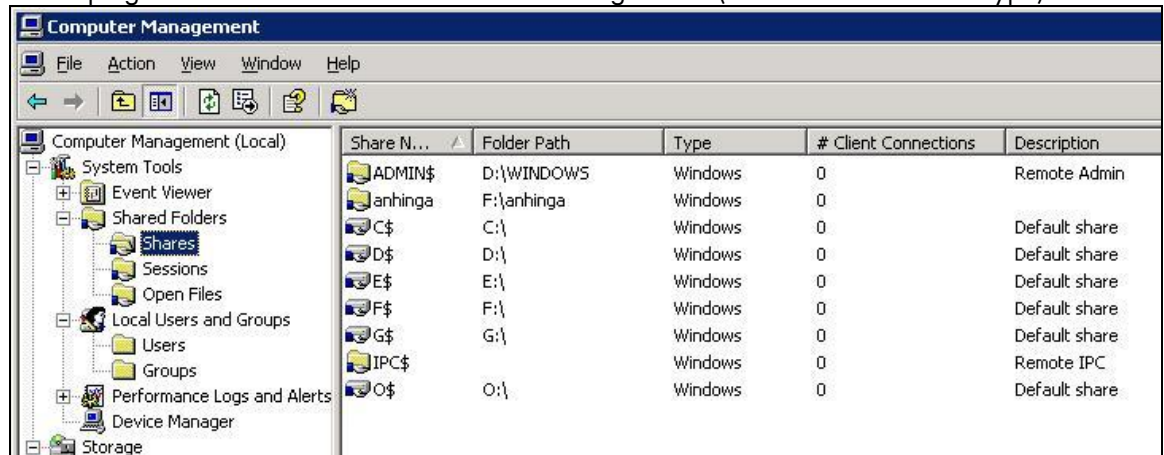
Limiting remote file shares

Keep file shares of any kind on any directory at a minimum to prevent sensitive security information from being exposed. Limit remote file shares through the Microsoft Manage menu:

1. Right-click **My Computer**, and select **Manage**.



2. Expand the Shared Folders directory, and select the **Shares** directory. HP highly recommends keeping these shares to a minimum and restricting access (both users and access type).



Share N...	Folder Path	Type	# Client Connections	Description
ADMIN\$	D:\WINDOWS	Windows	0	Remote Admin
anHINGA	F:\anHINGA	Windows	0	
C\$	C:\	Windows	0	Default share
D\$	D:\	Windows	0	Default share
E\$	E:\	Windows	0	Default share
F\$	F:\	Windows	0	Default share
G\$	G:\	Windows	0	Default share
IPC\$		Windows	0	Remote IPC
O\$	O:\	Windows	0	Default share

Firewalls and DMZs

In server environments, there can be various levels of security, ranging from “behind the firewall” (usually a trusted and safe environment) to “outside the firewall” (the public Internet). Some server environments have an in-between area, often designated as a DMZ. HP recommends placing your management servers (HP SIM and VPM servers) completely within your safest region because sensitive information is stored on these systems.

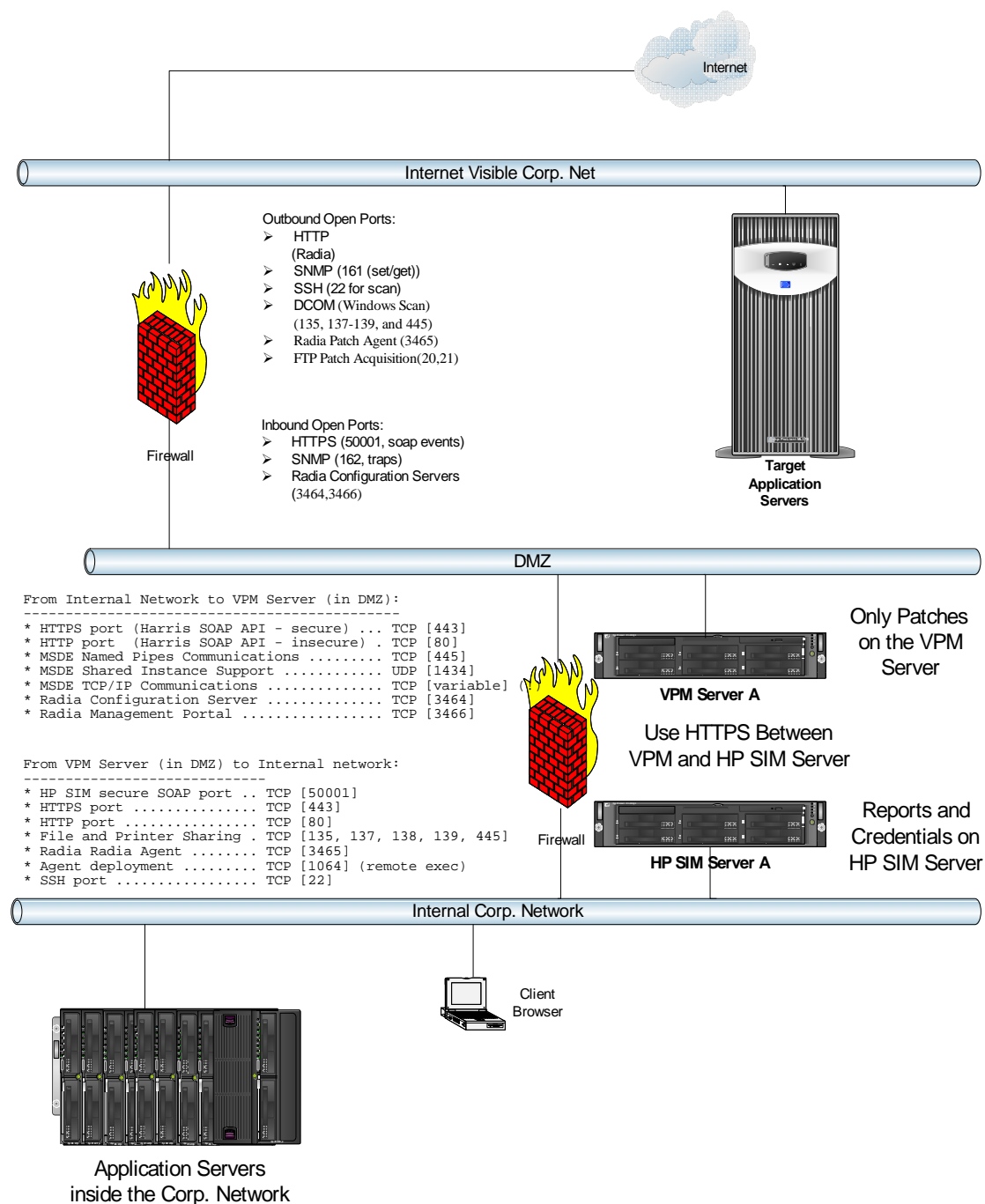
The following sections describe three sample configurations, which assume that WMI Mapper is residing with HP SIM and the client browser resides on the corporate network. The distributed model, represented as Configuration A, might fit well in the DMZ model because the HP SIM server can be secured inside the corporate firewall, while the VPM server is located in the DMZ. Because the majority of sensitive information is located on the HP SIM server, HP recommends keeping that server in the most secure environment. The VPM server receives orders from the HP SIM server and houses the patches acquired from the operating system vendors. However, the VPM server does retain a minimal amount of sensitive information and should not be exposed to a hostile Internet environment. Configuration B is the simple single-node configuration, with the majority of the target systems located inside the firewall, while a few target systems are located outside the firewall. Configuration C introduces the external patch acquisition option from Vulnerability and Patch Management Pack 1.10.

Configuration A

Configuration A consists of the VPM server in a DMZ and the HP SIM server in the corporate network. This configuration illustrates that you can separate the VPM server and HP SIM server for practical reasons, such as:

- Acquiring patches outside the corporate network
 - To acquire patches and updates, external FTP and HTTP access to the patch vendors (such as Microsoft, HP, and Red Hat) is required. Because many facilities do not allow files to be downloaded through their firewalls and proxies, especially on their corporate networks, it might be necessary to place the VPM server in the DMZ where patch acquisitions can be performed without risking exposure to your internal corporate network HP SIM server.
- Minimizing the open ports in your corporate firewall
 - Because the VPM server is outside the corporate network firewall, the server can manage from the DMZ and beyond without affecting the corporate firewall traffic load. Ports on the corporate firewall do not need to be open to perform scans from and beyond the DMZ.
 - The VPM server can also reach out to operating system vendor websites and acquire patches without requiring another open port in the corporate firewall.
- Minimizing the traffic through your corporate firewall
 - FTP traffic for patch acquisition and not on your corporate network.
 - Patch traffic to targets in the DMZ and outside the firewall is not on your corporate network.
- Keeping sensitive information inside your corporate network
 - Easily secure your communications channel from the VPM server to HP SIM server using HTTPS.
 - Sensitive persistent target information, such as vulnerability reports, patch reports, and target credentials, is stored on the HP SIM server inside your corporate network.
 - Client access to the HP SIM server can be further restricted using SSL with the client browser.

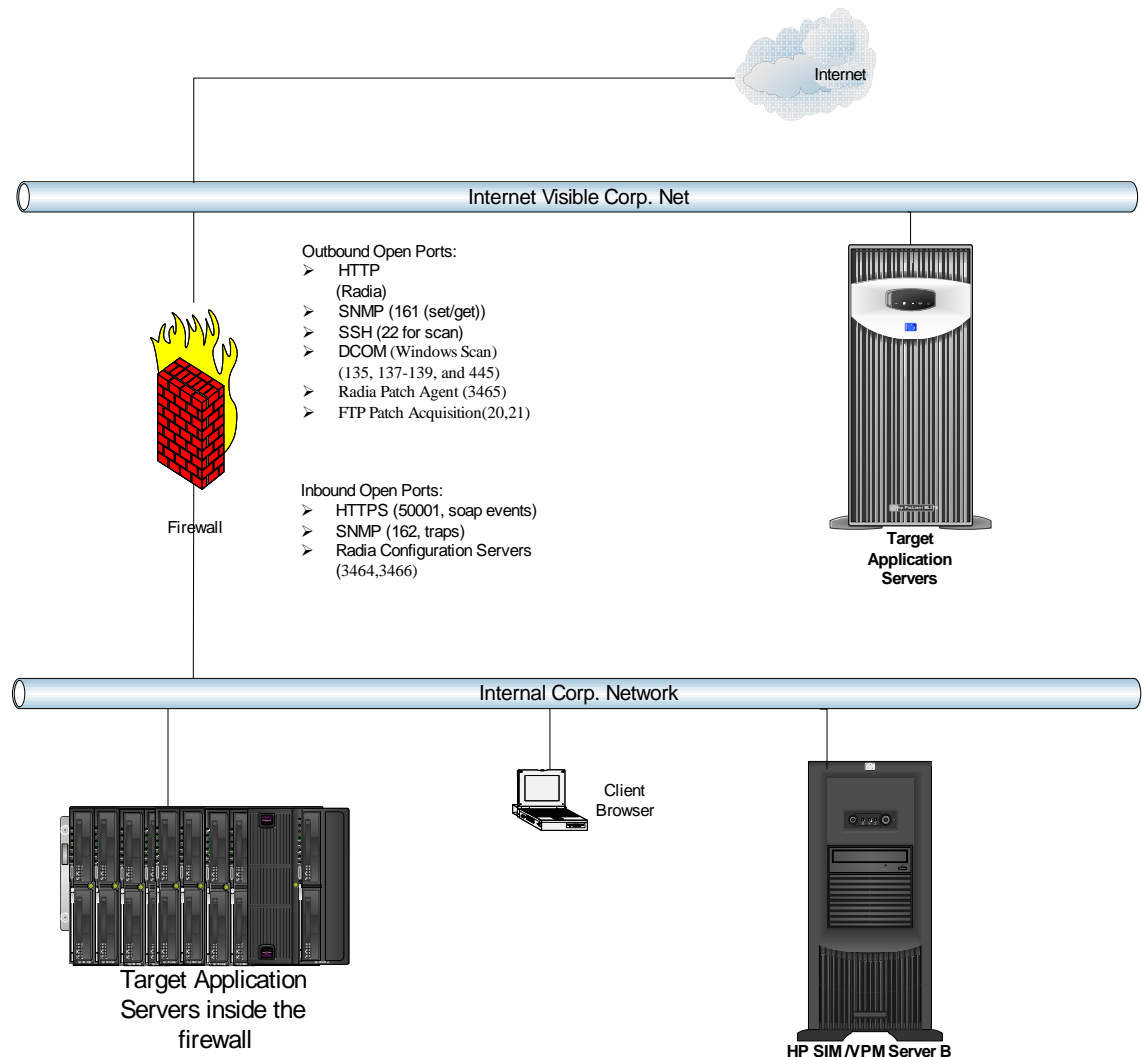
Figure 7. Configuration A



Configuration B

Configuration B consists of the VPM server and HP SIM server on a single system inside the corporate network. This configuration is best when trying to lock down the HP SIM/VPM server. Because all components are located on one node, there is a single focal point of securing the sensitive information of the target systems. It requires less overall server maintenance at the expense of potentially opening the firewall to perform Vulnerability and Patch Management Pack operations, such as scanning, patching, and patch acquisition.

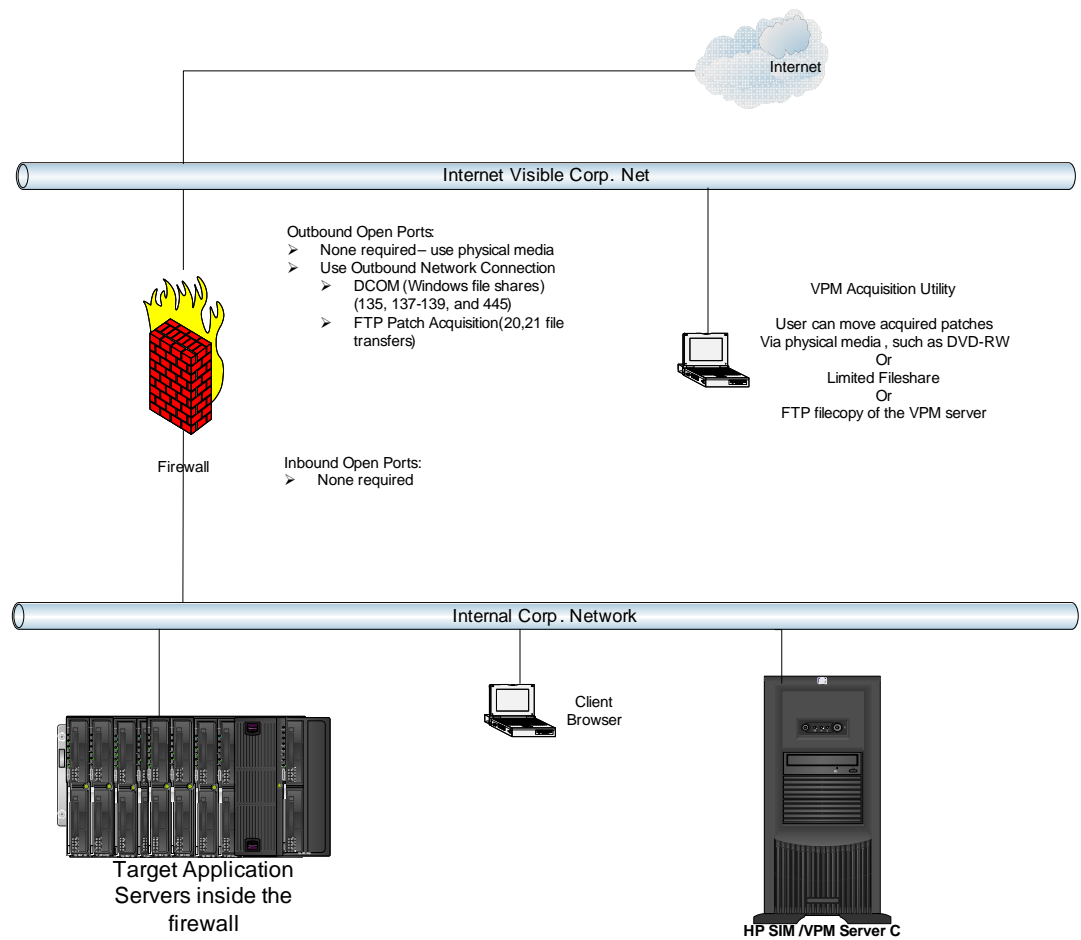
Figure 8. Configuration B



Configuration C

Configuration C consists of the VPM server and HP SIM server on a single system inside the corporate network, and the VPM Acquisition Utility located on a separate system that can reach operating system vendor websites and acquire patches via the Internet. This configuration, like configuration B, is suitable when attempting to lock down the VPM or HP SIM server, because all components with sensitive target system information are located on one node.

Figure 9. Configuration C



Vulnerability and Patch Management Pack firewall ports

HP SIM server

The following ports must be open on the HP SIM server.

Service	Port
HP SIM HTTP port	TCP [280]
HP SIM HTTPS port	TCP [50000]
HP SIM Web-Based Enterprise Management (WBEM)/WMI Mapper Secure Port	TCP [5989]
HP SIM SSH port	TCP [22]
HP SIM secure Simple Object Access Protocol (SOAP) port	TCP [50001]
SNMP	TCP/UDP [161]
SNMP traps	TCP/UDP [162]

VPM server

The following ports must be open on the VPM server.

MSDE

Service	Port
MSDE Named Pipes Communications	TCP [445]
MSDE Shared Instance Support	UDP [1434]
MSDE TCP/IP Communications	TCP [variable]*

For more information, refer to the following sources:

- <http://www.microsoft.com/sql/techinfo/administration/2000/security/winxpsp2faq.asp>
- <http://support.microsoft.com/default.aspx?kbid=839980>

Harris STATScanner Engine

Service	Port
HTTPS port	TCP [443]
HTTP port	TCP [80]
File and Printer Sharing for Microsoft Networks	TCP/UDP [135, 137, 138, 139, 445]

Radia Patch Manager

Service	Port
Configuration Server	TCP [3464]
Radia Management Portal	TCP [3466]

Target nodes

The following ports must be open on the target nodes.

Scanner access (target nodes)

Service	Port
File and Printer Sharing for Microsoft Networks	TCP/UDP [135, 137, 138, 139, 445]
Remote Registry service	TCP/UDP [135, 137, 138, 139, 445]
Default admin shares must be enabled	[IPC\$, ADMIN\$, C\$,]

HP SIM

Service	Port
SNMP	TCP/UDP [161]
SNMP traps	TCP/UDP [162]
HP ProLiant agents	TCP [2301, 2381, 49400]

Radia Patch Manager

Service	Port
Radia Agent	TCP [3465]
Agent deployment	TCP [1064] (remote exec)

Security relationship between Vulnerability and Patch Management Pack and target systems

Vulnerability and Patch Management Pack uses credentials with administrator level privileges to access remote systems. In some environments, it might be possible to spoof a remote system causing a man-in-the-middle attack. In a Windows environment, stealing the credentials used to access a remote system is highly unlikely because Windows authentication uses a one-way hashing function to encrypt the credentials. In Linux environments, OpenSSH provides a similar mechanism over an encrypted communications channel.

HP SIM has several security settings and features to detect and avoid target system spoofing. To avoid spoofing, you can use the HP SIM SSL and SSH features with the HP ProLiant server agents. HP SIM pushes an SSH SID to the target HP ProLiant server agent. If a rogue system is discovered, data collection failures occur because the rogue system cannot validate the SSH SID it received. If there is a failure in HP SIM data collecting and status polling the target because of security, it can indicate a rogue system. After HP SIM has discovered and authenticated the target, you can then proceed with Vulnerability and Patch Management Pack operations. You can further enhance security by creating SSL target system certificates and exchanging them with the HP SIM SSL certificate in the certificate store of each system. Both sides can be configured to accept SSL connections only to systems with which they have exchanged SSL certificates. For information about configuring these security features, refer to the HP SIM documentation.

The VPM server is the source of the following major functions:

- Vulnerability scanning
- Deploying patches
- Deploying configuration fixes

Each of these operations has different security requirements.

Vulnerability scan security

The VPM server probes the target system remotely. It does simple probes based on external TCP/IP port openings. However, to perform a significant in-depth analysis, the VPM server must inspect the system with more significant credentials. Generally, this inspection is done to find vulnerabilities inside the system, in case a system is penetrated. By finding and repairing these internal vulnerabilities, you attempt to minimize damage from any single system compromise.

The level of privilege given determines the amount of depth to which the scan can proceed. In HP SIM, Vulnerability and Patch Management Pack uses the WBEM credentials to enable the scan to have these privileges. WBEM credentials are set up system-wide for all HP SIM targets by selecting **Options>Protocol Settings>Global Protocol Settings** from the HP SIM menu or for individual systems by selecting **Options>Protocol Settings>System Protocol Settings**.

For example, the credentials used to scan configuration files allow Vulnerability and Patch Management Pack to read the etc directory but not to read the configuration files themselves (lmhosts). This configuration prevents any Windows fileshare configuration concerns.

Patch security

Patching requires full administrative software update privileges on the target systems. To install software, administrative privileges are required in the form of either Windows Administrative rights or the Linux RPM. In this version of the Vulnerability and Patch Management Pack, the VPM Patch Agent installation uses the WBEM credentials provided. The Radia Patch Agent installation verifies that the appropriate credentials are available to allow the agent to update target system software. If the agent has been installed successfully, sufficient privilege levels are available to perform the software updates as necessary.

Configuration fix security

Some vulnerabilities require configuration fixes. Automated configuration fixes require significant privileges. In this version of the Vulnerability and Patch Management Pack, configuration fixes are performed only on the Windows platform and use the provided WBEM credentials.

Vulnerability and Patch Management Pack patching and the Windows XP SP2 firewall

The Windows XP SP2 firewall requires additional ports to be opened for patching to function. The programs are `RADEXECD` and `NVDKIT`. If these two programs are disabled and removed from the exception list, Vulnerability and Patch Management Pack cannot reach out to the target devices and wake them to perform patch management tasks.

For more information

<http://www.hp.com/proliantessentials/vpm>

© 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. Linux is a U.S. registered trademark of Linux Torvalds. STAT is a registered trademark of Harris Corporation.

5983-0357ENA2, 05/2005